AN

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/756,346	01/08/2001	Henry Haverinen	442-010085-US (PAR)	6669

2512 7590 04/28/2005

PERMAN & GREEN
425 POST ROAD
FAIRFIELD, CT 06824

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/756,346	HAVERINEN ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 January 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13,15,17-20 and 22-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,12,13,15,17-20 and 22-30* is/are rejected.

7)☒ Claim(s) *11* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 1/26/2005 was received and considered.

2. Claims 1-13, 15, 17-20 & 22-30 are pending.

Response to Arguments

3. Applicant's arguments, see pp. 18-19 of REMARKS, filed 1/26/05, with respect to the rejection(s)of claim(s) 1-13, 15 & 17-20 under Federrath et al. have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Federrath and Sayers et al and hence this action will be made non-final.

4. Applicant's response (p. 19, ¶2) argues that there is no motivation to combine the references of record. However, Federrath teaches basic security in a GSM system, including authentication. Menezes teaches a detailed cryptographic approach to challenge-response (strong) authentication that prevents certain chosen-text attacks. Therefore, it would have been obvious to combine the references. Further, Sayers teaches a mobile communication system, which operates partly using the GSM protocol to enable mobile users (of GSM) to access voice and data systems from an IP-based network.

5. Upon further consideration of the specification, specifically Fig. 1 as Applicant's response has pointed out, the objection to the specification regarding the subject matter of claim 5 has been withdrawn.

6. In light of Applicant's amendments to claims 9 & 15, the objections set forth in the previous Office Action are withdrawn.

7. In light of Applicant's amendments to claims 4 & 12, the rejections under 35 U.S.C. §112 ¶2, set forth in the previous Office Action, are withdrawn.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 24, it is unclear whether "the at least two challenges" is referring to "at least two challenges corresponding to the mobile node identity" or "to form the cryptographic based on at least two challenges", or both.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 3-5, 8-10, 13, 19, 20, 22 & 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Protection in Mobile Communications" by **Federrath**, in view of U.S. Patent 6,539,237 to Sayers et al. (**Sayers**) in view of Handbook of Applied Cryptography by Menezes et al. (**Menezes**).

Regarding claims 1, 3-4, 9-10, 13, 19, 20, 22 & 28-30, Federrath discloses providing the mobile node/station with a mobile node identity/TMSI and a shared secret/Ki specific to the mobile node identity/TMSI and usable by a telecommunications network/home network (Fig. 1, p. 5), sending the mobile node identity/TMSI from the mobile node to the network/visited network, providing the network/visited network with authentication information usable by the telecommunications network/home network, the authentication information comprising a challenge/RAND and a session secret/Kc corresponding to the mobile node identity/TMSI and derivable using the challenge/RAND and the shared secret/Kc (Fig. 1, p. 5), sending the challenge/RAND from the network/visited network to the mobile node/station (Fig. 1, p. 5), generating at the mobile node the session secret/Kc and a first response corresponding/SRES to the challenge/RAND, based on the shared secret/Ki (Fig. 1, p. 5), sending the first response/SRES to the packet data network, and checking/authenticating the first response for authenticating the mobile node (Fig. 1, p. 5). Federrath lacks the visiting network being specifically a packet data network. However, Sayers teaches that to as wireless technology becomes more popular, companies desire to let workers increase mobility and access all voice and data information via wireless networks (col. 6, lines 58-65). Sayer's system comprises a private wireless network (Fig. 2) where mobile stations/phones communicate with protocol converters (P-BTS) that communicate with an IP network, such as the Internet (Fig. 2, #24) through a protocol interface (Fig. 2, #28-1) (see also col. 9, lines 26-65). Further, Sayers teaches that the software of the P-BTSs provide support for call connection in the wired protocol (col. 10, lines 49-62). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Federrath to allow the mobile units to interact with a

wired network, such as an IP network. One of ordinary skill in the art would have been motivated to perform such a modification to allow users to access all voice and data information via wireless networks, as taught by Sayers (Fig. 2, col. 6, lines 58-65, col. 9, lines 26-65 & col. 10, lines 49-62). As modified, Federrath lacks providing the mobile node with a protection code, sending the protection code with the mobile node identity/TMSI, forming cryptographic information using at least the protection code and the session secret, sending the cryptographic information with the challenge to the mobile node/station and checking at the mobile node the validity of the cryptographic information using the challenge and the shared secret. However, Menezes teaches that random numbers can be used in challenge-response mechanisms to provide timeliness assurances and avoid certain replay and interleaving attacks (§10.3.1 (i)). Menezes teaches that nonces can be used to provide timeliness guarantees where a receiving party (network) creates a response (cryptographic information) that depends both on a secret/Kc and the challenge/nonce (protection code) (§10.3 & §10.3.1 Background). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to provide the mobile node with a protection code/nonce, send the protection code/nonce with the mobile node identity/TMSI, form cryptographic information/nonce verification using at least the protection code/nonce and the session secret/Kc, send the cryptographic information/nonce verification with the challenge/RAND to the mobile node/station and check at the mobile node the validity of the cryptographic information/nonce verification using the challenge/RAND and the shared secret/Ki. One of ordinary skill in the art would have been motivated to perform such a modification to distinguish one protocol instance from another and to prevent certain chosen-text attacks in challenge-response protocols, as taught by Menezes (§10.3 & §10.3.1).

Regarding claim 5, Federrath, as modified above, discloses a link not being a link of the telecommunications network (visited network) (p. 5, Fig. 1).

Regarding claim 8, Federrath discloses obtaining a second response/SRES' by the telecommunications network/home network, and using the second response in the checking/(auth.result =?) the first response (p. 5, Fig. 1).

12. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers** and **Menezes**, as applied to claim 1 above, in further view of "The Network Access Identifier" by Aboba et al. (**Aboba**). Federrath, as modified above, lacks forming a Network Access Identifier from the subscriber identity/TMSI as the mobile node identity. However, Aboba teaches that the network access identifier is known in the art as an identifier for a user, to be used in roaming and to assist in routing an authentication request (§2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to form a network access identifier as the mobile node identity by the mobile node, from the subscriber identity. One of ordinary skill in the art would have been motivated to perform such a modification to assist in routing an authentication request, as taught by Aboba (p. §2.1).

13. Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers** and **Menezes**, as applied to claim 1 above, in further view of U.S. Patent 5,537,474 to Brown et al. (**Brown**). Federrath, as modified above, discloses using a Subscriber Identity Module, but lacks using it for the providing the mobile node with the mobile node identity and generating the session secret. However, Brown teaches that the mobile device in the

GSM system includes a SIM, programmed with the subscriber identity and shared secret/Ki, which calculates the session secret/Kc (col. 5, line 26 – col. 6, line 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the SIM for the providing the mobile node with the mobile node identity and generating the session secret. One of ordinary skill in the art would have been motivated to perform such a modification to conform to the GSM standard, as is well known in the art, and taught by Brown (col. 5, line 39 – col. 6, line 3).

14. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers** and **Menezes**, as applied to claim 1 above, in further view of "Internet Key Exchange (IKE)" by Harkins et al. (**Harkins**) in further view of Applied Cryptography, Second Edition by **Schneier**. Federrath, as modified above, lacks generating a session key for Internet Key Exchange, wherein the shared session key is based on the at least one session secret and the at least one challenge. However, Harkins teaches that Internet Key Exchange is a protocol used to establish authenticated keying material in IPSec (§1 & §2), which is authenticated using a pre-shared key (§5.4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a session key for Internet Key Exchange. One of ordinary skill in the art would have been motivated to perform such a modification to use IPSec, as taught by Harkins (§1-2 & §5.4). As modified, Federrath lacks the session key being based on the session secret and at the challenge. However, Schneier teaches that a 'salt' is a random string applied to a password to make it more difficult to find using a dictionary attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was

made to 'salt' the session secret/password with the challenge/random string. One of ordinary skill in the art would have been motivated to perform such a modification to make the session secret more difficult to find using a dictionary attack, as taught by Schneier (pp. 52-53).

15. Claims 15, 17, 18 & 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers**, **Menezes** and WO 01/41470 to Abrol et al. (**Abrol**).

Regarding claims 15, 17, 18 & 26-27, the claims are substantially equivalent to claim 1, but lack a gateway/network entity acting as an interface. However, Abrol teaches that by using a data service node/gateway that supports authentication between a mobile node and an authentication server, the benefit of providing authentication for a diverse set of mobile stations in a wireless network is gained (p. 3, ¶2-3). The data service node/gateway performs authentication techniques for the mobile station; otherwise, an authentication server is accessed (p. 3, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use an authentication gateway/data service node to authenticate mobile stations. One of ordinary skill in the art would have been motivated to perform such a modification to provide authentication for a diverse set of mobile stations in a wireless network, as taught by Abrol (p. 3, ¶2-3).

Regarding claim 27, Federrath discloses the mobile node being integrated with a mobile station (Fig. 1) and a terminal part providing the subscriber identity and shared secret to the mobile node and mobile station

16. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers**, **Menezes** and **Abrol**, as applied to claim 15 above, in further view of **Aboba**. Federrath, as modified above, lacks forming a Network Access Identifier from the subscriber identity/TMSI as the mobile node identity. However, Aboba teaches that the network access identifier is known in the art as an identifier for a user, to be used in roaming and to assist in routing an authentication request (§2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to form a network access identifier as the mobile node identity by the mobile node, from the subscriber identity. One of ordinary skill in the art would have been motivated to perform such a modification to assist in routing an authentication request, as taught by Aboba (p. §2.1).

17. Claim 25 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Federrath** in view of **Sayers**, **Menezes** and **Abrol**, as applied to claim 15 above, in view of **Harkins** and **Schneier**. Federrath, as modified above, lacks generating a session key for Internet Key Exchange, wherein the shared session key is based on the at least one session secret and the at least one challenge. However, Harkins teaches that Internet Key Exchange is a protocol used to establish authenticated keying material in IPSec (§1 & §2), which is authenticated using a pre-shared key (§5.4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a session key for Internet Key Exchange. One of ordinary skill in the art would have been motivated to perform such a modification to use IPSec, as taught by Harkins (§1-2 & §5.4). As modified, Federrath lacks the session key being based on the session secret and at the challenge. However, Schneier teaches that a 'salt' is a random string

applied to a password to make it more difficult to find using a dictionary attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to 'salt' the session secret/password with the challenge/random string. One of ordinary skill in the art would have been motivated to perform such a modification to make the session secret more difficult to find using a dictionary attack, as taught by Schneier (pp. 52-53).

Allowable Subject Matter

18. Claim 11 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

19. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks
Washington, DC 20231

Or faxed to:

(703)746-7239 (for formal communications intended for entry)

Or:

(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
April 18, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100